Information Security

Creating and Maintaining a Secure Computing Environment

Presented by
The State of Utah
Department of Administrative Services
Division of Information Technology Services
Computer Security Group

Information Security

Director's Message

State information and information systems are recognized as critical and important State assets. We must ensure that information and information systems are properly protected from a variety of threats, including error, fraud, embezzlement, improper disclosure, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster.

To assist with this process of protection, the Division of Information Technology Services has established a security awareness program. This program will cover virtually all aspects of information security, including requirements from the State Information Security and Acceptable Use policies.

ITS management takes security seriously and urges you to do the same, and asks you to cooperate with us in creating and maintaining a secure computing environment.

Stephen W. Fulling
Director

Information Security

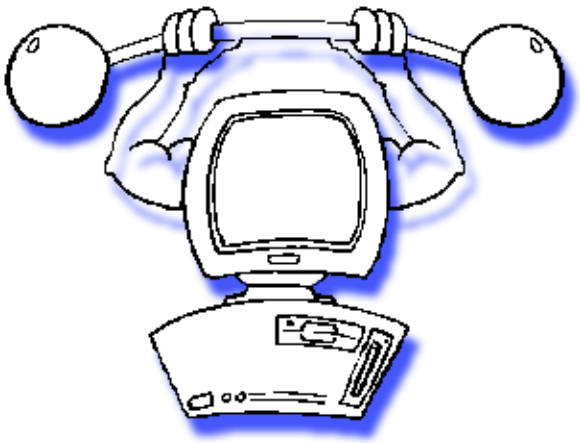
What is Information Security?

Information Security is:

~ a combination of policies and procedures
~ designed to protect equipment, data, and applications
~ from unauthorized disclosure, modification, or loss.

Information Security

Advances in technology,
the widespread use of personal computers,
and the Internet,
make it easy for more people
to access and manipulate information.



Information Security

Who is responsible?

The Computer Security Group is concerned
with protecting both the equipment
and the information it contains.

Access to both computer information
and computer applications
must be controlled to ensure only authorized users have access.

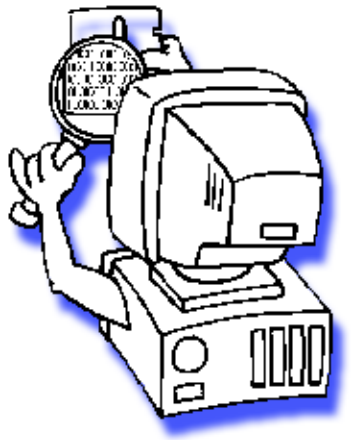
Everyone can help prevent unauthorized individuals
from accessing our information systems.

Information Security

What can you do?

When you leave your work area:

~ Be aware of the visibility of data on your PC or terminal screen.
~ Use a password protected screen saver, or lock your PC.
~ Lock up sensitive reports and other computer media.

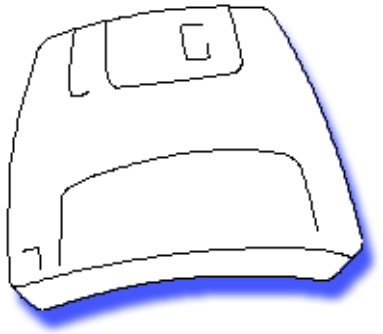


Information Security

~ When no longer needed, printed reports should be shredded or placed in confidential bins for burning.

~ Data on magnetic media should be overwritten or degaussed. (Files that are deleted are ***not*** erased and can still be recovered.)

~ If you are a supervisor, notify the Computer Security Group when employees transfer or are terminated.



Information Security

Password Protection

Having a good password is the best way for you to prevent unauthorized access.

Protect your password by:

~ Choosing a password that is hard to guess.
Hint: Mix letters and numbers or special characters.
~ Use longer passwords.
They are more secure. Six to eight characters is suggested.
~ Be sure that your password does not appear on printouts.

Information Security

Password Protection

~ Do not share your password with anyone.

~ Do not use a password that can be closely identified with you.
(Your address, pet's name, nickname, spouse's name, make of car you drive, etc.)

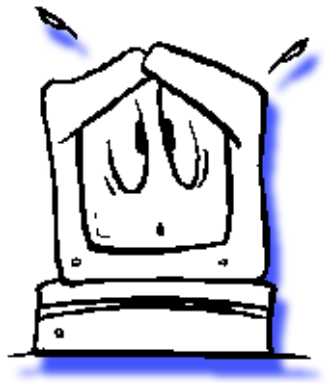
~ Do not tape passwords to desks, walls, or terminals.
Commit your password to memory.

Information Security

What about computer viruses?

A computer virus is a program
that replicates itself
and attaches itself to other programs.

Virus protection software can prevent known viruses
from being installed on your computer
and from spreading to others.



Information Security

Symptoms of a Computer Virus

Symptoms of a virus include, but are not limited to:

~ Files that Appear or Disappear
~ Data is Changed
~ Disk Space or Memory Changes
~ "A" Drive Light Flashes when the Drive is Empty
~ System Slows Way Down
~ Unusual Video Displays Appear
~ Workstation Reboots Unexpectedly
~ File Time Stamps Change

Information Security

Suspect a virus?

These symptoms may be related to other issues or problems ...

... but if you suspect a virus, contact the ITS Help Desk immediately by calling :

801-538-3440

Information Security

Internet Access

The Internet provides:

~ the ability to communicate with others, and,
~ access information throughout the world.

There is little control over the information available there:

~ Some is Controversial
~ Some has Little Value to Employees or the State

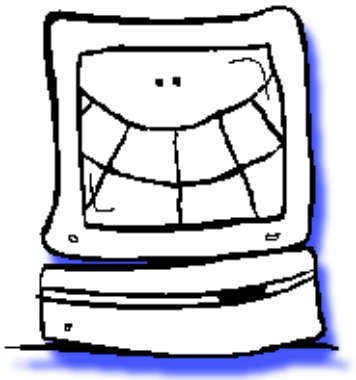
Information Security

Internet Filtering

Filtering products allow restrictions on the types of Web pages that can be viewed from the State network.

Some examples of prohibited sites include:

- ~ Pornography
- ~ Militia Groups
- ~ Weapons
- ~ Bomb Making Sites



Information Security

System Monitoring

Directors, network and computer operations personnel,
and system administrators monitor
the Internet, email, and network systems.

It should be assumed that the content of these systems
will be seen by these authorized individuals.

Don't say, do, write, view, or acquire anything
that you wouldn't be proud to have everyone in the world learn about
if the records are laid bare.

Information Security

Who do I call for help?

If you need assistance with:

~ Password Resets
~ System Access
~ Any Security Related Issues

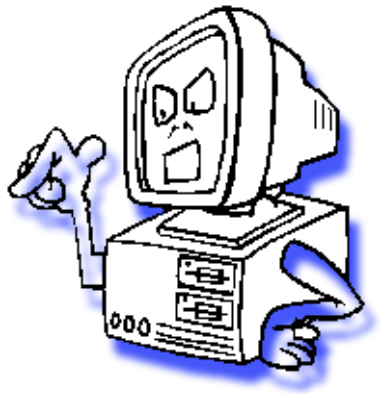
Please Call the ITS Help Desk
at
801-538-3440

Information Security

Acceptable Use Policy

The State of Utah
Information Technology Resources Acceptable Use Policy
can be viewed in its entirety at:

http://cio.utah.gov/policiesstandards/approved_docs/acceptableusepolicy.htm



Information Security

The End

Remember to Create
and Maintain
a Secure Computing Environment

Information Security

Please Print Out , Read, and Sign this Page

I understand that I am responsible for knowing the content of the Acceptable Use Policy for ITS and will comply with the parameters outlined therein. I understand that this document will be placed in my permanent personnel file.

Employee Signature Date